

REMARKS

Claims 1-4, 6-12, 14, 19, 21-26, and 28-30 were pending in the patent application. By this amendment, Applicants have canceled Claims 14-19. The Examiner has rejected Claims 1-3 (or 4), 6-12, and 28-30 under 35 USC 102(e) as anticipated by the teachings of the Isikoff patent; and, has rejected Claims 14-19 and 21-26 under 35 USC 103 as unpatentable over the combined teachings of Isikoff and Nerlikar. Based on the amendments and remarks set forth herein, Applicants respectfully assert that the remaining claims, Claims 1-4, 6-12, 21-26, and 28-30 are allowable over the cited art.

The present invention relates to a portable computer having a radio frequency identification chip (RFID chip) and a radio frequency antenna (RF antenna) security device incorporated therein. The computer apparatus and method provide for detection of removal of the RF antenna security device and denial of access to the computer if it is determined that removal of the RF antenna security device was unauthorized. Under the present invention, unlike the prior art, the security device can optionally be legitimately removed from the portable computer with

JA998-227

-12-

authorization, and access to the computer will not be denied. The computer has a first storage area for storing data including an antenna history bit indicating whether a security device was ever attached to the computer. That storage area is capable of storing information received from an RF source even when the computer is not powered up. Moreover, the invention further provides for protection of that stored data (i.e., prohibiting access to change that stored data) so that an unauthorized user cannot alter the original stored information. Upon successive monitoring by the CPU, or powering up of the computer, the stored data is accessed to determine whether a security device was ever attached to the computer. Further, it is dynamically determined if the security device is presently attached to the computer. If the security device is not presently attached, and removal was not legitimate (as determined, for example, by entry of an authorized password), access to the computer is denied. If, however, it is determined that removal of the security device was legitimate, access to the computer is permitted, and the authorization information is stored for future reference.

The Isikoff patent is directed to a computer antenna which is used both for communication and security. If the

computer is stolen, the antenna signal can be traced to locate the computer. Isikoff provides for the antenna to be activated as a security device when unusual activity is detected. In addition, Isikoff mentions, although does not provide implementation details for, actuating internal security protocols, such as erasing the hard drive, in response to the unusual activity. Applicants respectfully assert, however, that Isikoff does not teach or suggest the invention as claimed.

Isikoff does not provide a first storage location, capable of storing antenna history bit data, even when the power is not turned on, wherein the stored data indicates whether an RF antenna security device was ever attached to the computer. Isikoff does not teach or suggest that antenna history data be stored or accessed in order to verify whether an antenna should be connected. Rather, Isikoff detects a misentered password (Col. 9, lines 11-13) or may test circuitry wired to the antenna (Col. 4,, lines 43-44) in order to determine that the computer has been stolen or tampered with. Further, Isikoff does not provide any details regarding legitimate removal of, or disabling of, its antenna, use of a password to allow legitimate removal of its antenna, or storage of information regarding

legitimate removal of its antenna. Isikoff expressly teaches that the antenna is integral to the computer unit and that any tampering is unauthorized. Finally, while Isikoff does suggest disabling some operation of the computer when tampering or removal is detected, Isikoff does not teach or suggest that access to the computer is prohibited unless the removal of the antenna is verified as appropriate (i.e., the antenna history bit indicates that no antenna was attached) or authorized (i.e., that removal was appropriate as verified through use of a password in conjunction with the antenna history bit). Since Isikoff's RF pager system is designed to transmit to outside receivers, Isikoff clearly does not teach or suggest that its RF antenna communicates data to an internal RFID chip even when the computer is not powered on.

It is well established under U. S. Patent Law that, for a reference to anticipate claim language under 35 USC 102, that reference must teach each and every claim feature. Since the Isikoff patent does not teach RFID chip and storage means or steps for storing data comprising at least an antenna history bit about original attachment of an RR antenna security device, does not teach that said storing can be conducted without powering on the computer, does not

teach accessing the stored data and determining if a security device has been removed based on accessing that data, and does not teach determining if removal was authorized, with storage of authorized removal data, it cannot be maintained that the Isikoff patent anticipates the invention as claimed.

The Examiner has additionally cited the Nerlikar patent for its teachings related to a PCMCIA card with RFID and RF antenna. Applicants respectfully assert that neither the Isikoff patent nor the Nerlikar patent provide any teaching or suggestion which would motivate one to modify Isikoff with Nerlikar. Isikoff provides its RF pager system exclusively for the purpose of communicating the location of the computer to outside receivers. There is no teaching or suggestion that Isikoff should have an RFID chip within the computer for communicating with the RF pager system. It would not be logical to suggest that the Isikoff computer transmit its RF paging signals to itself, since the signal generating computer cannot locate itself. Clearly, therefore, it would not be logical to modify Isikoff with the PCMCIA card of Nerlikar.

Applicants further assert that, even if one were motivated to modify Isikoff with Nerlikar, one would not

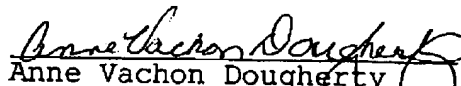
arrive at the invention as claimed. Neither Isikoff nor Nerlikar teaches or suggests storing at least an antenna history bit, taking steps to prohibit changing the antenna history bit, or using an antenna history bit to determine if an antenna which had previously been connected to the computer is currently connected to the computer, it cannot be maintained that the combination of references obviates the claim language.

Based on the foregoing amendments and remarks, Applicants respectfully request entry of the amendments, reconsideration of the amended claim language in light of the remarks, withdrawal of the rejections, and allowance of the claims.

Respectfully submitted,

J. Tanaka, et al

By:

  
Anne Vachon Dougherty  
Registration No. 30,374  
Tel. (914) 962-5910